An engineer's history of US and multilateral export controls and their application to the modern space industry

Juno Woods[1,*]

Open Lunar Foundation, 399 Webster Street, San Francisco, CA 94117, United States

Abstract

Export controls represent a critical barrier in the space industry, one which is poorly understood by most engineers. These laws and regulations, written long before there existed a commercial space industry, have impacted both the industry and international collaboration enormously. Moreover, they contradict a fundamental tenet for many engineers — that their work is a form of creative expression and thus, in the United States, worthy of First Amendment protections. In this manuscript, I present a history of multilateral arms control regimes, focusing on non-binding agreements such as COCOM, the Wassenaar Arrangement, and the Missile Technology Control Regime, their relationships with ITAR and EAR in the United States, and the historical context under which these policies were developed. Next, I discuss export control violations in the 1990s involving Hughes and Space Systems/Loral which exerted an outsized influence on the aerospace industry's attitude toward ITAR and EAR, the economic damage dealt to the commercial space industry, and the subsequent series of reforms that led to the modern-day regime. Third, I explore the jurisprudence around these regulations and laws, particularly as they relate to the First Amendment and the activities of engineers. Finally, in the context of the New Space revolution, I recommend changes to these policies that encourage a sustained and peaceful presence in space, with an eye toward cultures of innovation (e.g. open source), international standardization, and domestic competitive advantage.

Keywords: export controls, ITAR, EAR, COCOM, Wassenaar Arrangement, Missile Technology Control Regime, First Amendment, China, open source software, open hardware, open standards

1. Introduction

The set of laws, regulations, and international agreements known as export controls touch nearly every aspect of the civil space industry: hiring, academic publishing, international collaboration, even workplace architecture. While the costs of such policies were minuscule next to government-era space projects like Apollo and the Space Shuttle, the regulatory burden — due largely to the fixed costs of regulation [1] — is more significant for modern 'New Space' companies such as SpaceX, Rocket Lab, and Astra, which historically have worked with smaller budgets. Recent international agreements such as the Artemis Accords push for international cooperation in humanity's quest for lunar settlement, yet don't attempt to solve the problem of international arms control regimes that limit such cooperation.

In this article, I attempt to vertically integrate three aspects of export controls. I begin by exploring the history of the various formal and informal agreements that generally aim to balance conflict prevention and non-proliferation with peaceful use. Next, I discuss the evolution of US laws and regulations which often exceed the requirements of such multilateral arms control regimes; I consider the Cold War terroir first, and secondly, the more recent historical developments, along with practical implementation issues amid evolving sociological and information technologies. Finally, I discuss some of the US jurisprudence around export controls, primarily in their intersection with free speech, as I encounter many engineers who view their work as expressive in the First Amendment sense (a perspective which is often at odds with legal precedent).

It is my hope that this work will offer aid in several key areas. First and foremost, to consider changing a pre-existing system, one must understand its origins and underlying motivations; and international collaboration in the space domain requires some policy shifts. Secondly, I hope to provide New Space companies with insights into export control from a perspective other than that of legal scholarship — that is, written by an engineer, whose primary responsibilities don't include mitigation of legal risks. Thirdly, I aim to provide insight on the effects of these policies on collective invention in the space industry, including the open science movement, free (libre) software and open source software, open hardware, and other types of pre-competitive collaboration.

*Corresponding author

Email address: juno@translunar.io (Juno Woods)

[1]Director of Engineering Research & Strategy (emeritus), Open Lunar Foundation

2. The Cold War and arms control regimes

While wartime export controls were common throughout early United States history, the 1940 Export Control Act represented the nation's first peacetime trade controls (albeit looking down the barrel of war). The law included items of strategic military importance as well as commercial items, mirroring the modern regulatory distinctions between 'defense articles' and 'dual-use' items. The United States joined the Second World War shortly thereafter, and the Act was extended and updated periodically.[2] It provided broad authority to the executive branch to set penalties, issue export licenses, and determine the contents of the control lists. Moreover, it exempted the rule-making procedures from most common forms of public and judicial review. It also governed technical data. [2]

Following World War II, the United States pushed Western Europe for a multilateral agreement on export controls over the period between 1945 and 1949 [3]. Parties to this informal agreement were collectively known as the Coordinating Committee on Export Controls, or COCOM.

Like the Export Control Act, COCOM had dual objectives. First, it aimed to strategically prevent equipment for manufacturing armaments from flowing to communist nations, and secondly, it attempted to impose an "economic 'iron curtain"' as described in NSC 68 [4]. This arrangement included at least the US, the UK, France, Belgium, the Netherlands, Denmark, Canada, Luxembourg, and Germany [3], though accounts vary as to the exact membership at the time of founding, and others joined over time.

COCOM generally required unanimity to add an item to its control list, and countries wishing to export controlled items agreed to seek permission from fellow COCOM members. The three lists the organization maintained were known as the Atomic List, the Munitions List, and the Industrial List [5]. While COCOM never published these lists, nations often copied them nearly verbatim in setting their own export controls.[3] The US first regulated exports to Soviet Bloc countries in late 1948 [7], but the direction of information flow (whether to COCOM from the US or the other way around) is unclear, and regulatory authority was first granted to the Commerce Department for exports in early 1949 by the Export Control Act.[4]

From the fifties on into the sixties, anxieties about nuclear proliferation had grown in the minds of the public. While nuclear bombs were brought to bear in World War II, the invention of space launch technology in 1957 by the Soviet Union (Sputnik) and in 1958 by the United States (Explorer I) enabled these devices to be delivered ballistically, magnifying fears. In the third Nixon–Kennedy presidential debate in 1960, Senator John F. Kennedy expressed concern "that 10, 15, or 20 nations will have a nuclear capacity, including Red China, by the end of the Presidential office in 1964" [8].

As such, the years 1965–1968 saw the negotiation of the Treaty on the Non-Proliferation of Nuclear Weapons or NPT. The central bargain of the NPT was that non-nuclear-weapon states agree not to acquire nuclear weapons in exchange for the use of peaceful nuclear technology provided by nuclear-armed states. A key theme emerging from this period was the inherent challenge with all dual-use technologies, that their use or misuse depends often on the intent of those possessing them. The NPT was the first of three binding treaties on weapons technology, the others being the Biological Weapons Convention of 1972 and the Chemical Weapons Convention of 1993 [9] (outside the scope of this article). Yet the weaknesses in binding treaties would soon become apparent, owing in part to the rapid evolution of technology; less formal soft law arrangements like COCOM were far simpler to update over time.

The creation of another such non-binding multilateral export control regime, the Nuclear Suppliers' Group (NSG), was sparked by the 1974 testing of a 'peaceful nuclear device' by India. India had obtained a CANDU nuclear reactor and heavy water from Canada and the United States through President Eisenhower's 1953 'Atoms for Peace' program, an attempt to emphasize the peaceful uses of nuclear technology amid concerns about the nuclear arms race [10]. India, never having signed the NPT, was not bound by the treaty, and a need was seen for a supplier-side agreement to require acceptance of International Atomic Energy Agency safeguards before exporting to any non-nuclear-weapons state [11]. So-called 'full scope' safeguards (on the entire fuel cycle) would not be realized by the NSG until after the Gulf War in the 1990s [12], demonstrating the adaptability of such non-binding arrangements.

The International Traffic in Arms Regulations (ITAR) originated in the 1976 Arms Export Control Act (AECA; not to be confused with the earlier ECAs), which gave the executive branch the authority to regulate "defense articles (arms, ammunition, and implements of war), defense services, and directly related technical data." While the 1968 Foreign Military Sales Act authorized foreign aid in the form of defense services, the AECA was the first to *limit* the provision of defense services, and Congress left definition of this term up to the executive branch.[5] The Department of State was responsible for administering these

[2] Extensions in 1944, 1945, 1946, and 1947; re-enactment in 1949 with further extensions in 1951, 1953, 1956, and 1958.

[3] The British versions from 1954 onward are available at `https://evansresearch.org/cocom-lists/` [6].

[4] The US lists were said to be broader than the COCOM lists [2].

[5] Today, *defense services* are defined in 22 CFR 120.9(a) as

> (1) The furnishing of assistance (including training) to foreign persons, whether in the United States or abroad in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense arti-

regulations, though the Defense Department generally determined the contents of the control list [2], which is known as the US Munitions List, or USML. From passage of the 1976 AECA onward, the USML included all items listed in the MTCR annex except those separately regulated as dual-use items.

In 1969, amid the cooling of tensions known as detente, some in the US had hoped to deregulate trade between the East and West, and bring the US control lists in line with COCOM in the 1969 Export Administration Act (EAA) [2].[6] The Export Administration Regulations (EAR) were ultimately created by the 1979 EAA revision, and have generally been described as more complex than ITAR. The EAA authorized Commerce Department controls with several different justifications, all of which fell under the umbrella of dual-use technologies. Firstly, national security items were largely drawn from COCOM. Secondly, it permitted controls advancing foreign policy goals. Thirdly, controls might be used to ensure US access to resources. Interestingly, the regulations included a general license for published, scientific, or educational technical data, meaning that no export license was required for these data [2]. This exemption for information already available to the public remains in place today.

The eighties saw the creation of two new supply-side multilateral export control regimes, supplementing COCOM and the Nuclear Suppliers Group. The Australia Group (1985) dealt with chemical weapons, and is not discussed further in this article. The fourth, the Missile Technology Control Regime, was formed in 1987, and is especially impactful upon space technology. Whereas the NSG focused on nuclear technology, the MTCR attended to the delivery technology.

The Missile Technology Control Regime was a Reagan administration response to apprehensions relating to several missile and rocket tests, by South Korea, Iraq, and India, among others [13]. The purpose was to "reduce the risks of nuclear proliferation by placing controls on equipment and technology transfers which contribute to the development of unmanned, nuclear-weapon delivery services" [14], though later it expanded to include weapons of mass destruction generally. The MTCR had seven founding members, and has grown to thirty-five today. All of the items regulated by the MTCR have been incorporated into the USML. [7]

The end of the Cold War required a retargeting of the supply-side export control agreements away from the former Warsaw Pact states. 1993 saw the termination of COCOM, and its replacement by the Wassenaar Arrangement (WA) in 1996. Lipson [15] has argued that the WA differed from COCOM in several key respects. Firstly, the membership was significantly larger than that of COCOM and required consensus. Secondly, it offered greater transparency as compared to COCOM (including a website). Thirdly, it lacked the power to veto exports of controlled items, for which member states previously had to seek out authorization (though neither were COCOM's lists binding). The WA has been described as the weakest and least effective of the major multilateral export control regimes. Today, it controls many dual-use items, such as commercial communications and imaging satellites.

In order to understand ITAR and EAR, it's important to understand the motivations behind the arms control agreements that undergird these regulatory frameworks. Lipson [15] argued that the arms control regimes relate to shared identity and shared norms between member states. Joyner [16] called the regimes 'security communities,' though Beck and Jones [9] point out that regime members — unlike those of other security communities — don't necessarily view the threat of force against one another as unthinkable. Abbott and Snidal [17] distinguished between 'hard' and 'soft' law, arguing that these regimes are soft law, which are less threatening to nations' senses of national security and sovereignty, and more adaptable than treaties.

3. The evolution of modern US export controls

A key theme in and after the 1990s was that of growing technical capabilities of academia and private industry, whereas previously many of the controlled exports were much more closely tied to the US government. Space technologies, particularly communications satellites, bounced back and forth between the USML and the CCL (Commerce Control List) several times over the two decades subsequent to the end of the Cold War. With rocket technology still largely the domain of governments, inexpensive launches were in high demand among US companies, and this need often caused satellite manufacturers to turn to China.

Yet with the end of the Cold War, US national security concerns began to shift from the former Soviet Union to China. Zinger [18] has provided an excellent history of the policy aspects of export controls from the 1990s to around 2015, which begins with the explosion of three Chinese rockets carrying US commercial communications satellites. Companies such as Space Systems/Loral and Hughes were eager for a low-cost path to orbit, and believed they had found this in China Great Wall Industry

cles;

(2) The furnishing to foreign persons of any technical data controlled under this subchapter...whether in the United States or abroad;

(3) Military training of foreign units and forces, regular and irregular, including formal or informal instruction of foreign persons in the United States or abroad or by correspondence courses, technical, educational, or information publications and media of all kinds, training aid, orientation, training exercise, and military advice. (See also...)

[6] The EAA was itself a revision of the earlier ECA.

[7] According to ITAR, 22 CFR Sec. 120.29.

Corporation (CGWIC), a subsidiary of the PRC's main space contractor, China Aerospace Science and Technology Corporation (CASC).

3.1. Hughes Optus B2 and Apstar 2

The foundational events of modern export controls took place when Chinese Long March 2E rockets carrying US satellites — the Hughes Optus B2 on 21 December 1992 and the Hughes Apstar 2 on 26 January 1995 — experienced launch failures. Investigations by Hughes pointed to the fairings as the source of the accidents. According to the 1999 Cox report, confusion over jurisdiction and licensing requirements on the part of both Hughes and government officials led to Hughes relaying technical assistance for improving Long March fairings to China after both failures. In 1995, for example, the fairing — being a piece of the rocket — was regulated under ITAR, but a Commerce official, assuming it to be part of the satellite, mistakenly approved the disclosure. [19]

The nature of the technical data Hughes provided to China after the first failure makes for interesting reading. Hughes could not obtain insurance for launches subsequent to Optus B2 without a technical solution. The PRC was unwilling to acknowledge that the fairing was the cause, allegedly for political reasons. The approved but unlicensed transfer included two simple recommendations for changes to the fairing: "Add a bracket or block to prevent any possibility of overlap of the two fairing halves," and "Increase the strength of the rivets along the separation line" (which would prevent the fairing from opening prematurely). What Hughes officials viewed as fixes to design flaws, the government contended were improvements. In the process, Hughes likely revealed analysis methodologies. [19]

3.2. Loral Intelsat 708

On February 15, 1996, a similar fate befell the Loral Intelsat 708, aboard a Long March 3B. CGWIC asked a Loral official to chair an independent review committee. The official recruited experts from several US, German, and British aerospace companies, including Hughes. The PRC reported a broken wire in the inertial measurement unit (IMU) as the cause. The committee disagreed with the finding, however, and sent — without seeking US government review — a draft report suggesting two other possible causes, the second of which the PRC found to be the failure source. In essence, the disclosure led to the PRC discovering and correcting a failure in the Long March 3B guidance platform. [19]

Whereas the details of the Hughes launch failure disclosures were nuanced, the Intelsat review committee's alleged violation was straightforward and egregious. The Cox Report notes that "Loral was aware from the start of the Independent Review Committee's meetings that it did not have a license for the Independent Review Committee activity" (p. 109). The 200-page report included short-term and long-term recommendations. A US government interagency team noted particular concern around the exposure of Western diagnostic procedures to China. [19]

Much of the information shared with China was in the public domain at the time, leading Loral officials to believe that no license was required for these technical data. However, the Department of Defense believed that the review committee performed a "defense service."

> In general, a US citizen may transfer public domain information to a foreign national. However, such a transfer is not allowed if it occurs in the performance of a defense service, which is defined in Part 120 of the International Traffic in Arms Regulations. (p. 164)

Moreover,

> The expertise and experience of the person making the disclosure, and the circumstances of the disclosure, are important in determining whether a defense service has been performed through such a disclosure. As an example, simply giving a foreign national an article from the Encyclopedia Britannica is not an export requiring a license. If, however, the article is provided to a foreign national by an experienced engineer in the context of specific technical discussions, a defense service that requires a license may have been performed. [19]

The defense service claim is particularly interesting given that China's ballistic missiles were already sufficiently advanced that neither the CIA nor DOD believed the committee's improvements would benefit the program; China used a different guidance system and IMU aboard its missiles [19]. While the US had legislated (and regulated) above and beyond the requirements of the MTCR previously, in this case they had taken enforcement just as seriously. While the US was also concerned about analysis methodologies and engineering approaches being shared with the Chinese, these also were not covered in the MTCR.

The government charged Loral with 64 counts "of violating rules governing the transfer of sensitive technologies and underscored a prohibition on providing 'any technical assistance whatsoever' to Chinese authorities seeking to improve their capabilities" [20]. In a settlement, the company paid fines of $20M. Hughes' fines eclipsed these at $32M, perhaps because the failures had been systemic rather than at the level of an individual employee.[8]

3.3. Fallout and subsequent years

A month after the Long March 3B crash (and well before the formation of the independent review committee),

[8] The law allows for fines of $1M per count, plus ten years of jail time.

on 14 March, the Clinton administration announced that licensing authority for commercial communication satellite exports would be shifted from State to Commerce, in this case to incentivize China to participate more fully in the MTCR.[9] However, a Clinton re-election campaign fundraising scandal, connected to a former Commerce employee and the Chinese government, may have generated concerns about how the effort was motivated [22]. As Zinger [18] noted, the shift was short-lived; following the release of the Cox Report in 1999, Congress returned commercial satellite licensing to ITAR, and took away the president's power to determine satellite jurisdiction, where it remained for fourteen years. The United States became the only nation which treated all commercial satellites as munitions [23].

In 1997, the US had enjoyed a substantial majority of the satellite manufacturing market. Ten years later, it had lost that dominance, with foreign satellite manufacturers selling products they advertised as 'ITAR-free.' The Defense Department found that US companies had lost $2.35B of sales due to the ITAR licensing process. [24]

It took another six years for Congress to stem the flow. The Obama Administration proposed reforms to the USML with the manufacturing and technology sectors in mind in 2010, and a 2012 report by the State and Commerce Departments affirmed many of those reforms, acknowledging that many of the satellite technologies regulated under ITAR were available without such stringent controls from a number of other countries [23]. Goals of these reforms included unification of controls on a single list, under a single licensing agency, with only one agency handling enforcement [25].

In 2013, Congress finally returned to the executive branch the power it had taken in 1999, except as regarding China, North Korea, and state sponsors of terrorism. Zinger [18] argued that the 2013 reforms were both much-needed for the US commercial space industry and an abject failure in terms of their ability to prevent confusion about the split jurisdiction of certain exports, such as in the Hughes case.

The Export Control Reform Act (ECRA) of 2018 recognized economic security as a key goal.

> The national security of the United States requires that the [US] maintain its leadership in the science, technology, engineering, and manufacturing sectors, including foundational technology that is essential to innovation. Such leadership requires that United States persons are competitive in global markets. The impact of the implementation of this part on such leadership and competitiveness must be evaluated on an ongoing basis and applied in imposing controls...to avoid negatively affecting such leadership. [26, Section 1752(3)]

It also noted the ineffectiveness of unilateral export controls on items readily available abroad. Thirdly, the law emphasized the importance of small and medium-sized businesses [26]. Finally, the law further expanded executive power with regards to dual-use exports [25]. While these changes to federal law created the framework for regulatory improvements, only some of these have been realized.

While not specifically related to export controls, Congress further limited collaborations between the US and China in 2011, via an amendment by Rep. Frank Wolf, over espionage [27] and human rights concerns — a policy which remains in force [28], and which the Biden administration has supported making permanent [29]. The law required Congress to specifically authorize any interactions that involved the PRC among NASA, the Office of Science and Technology Policy, or the National Space Council. The effort does not appear to have slowed China, which has successfully landed multiple spacecraft on the Moon, including one on the far side.

Perhaps the largest impact of the modern export control regime has been on hiring. The Defense Department has noted aerospace and defense companies face a skills gap in the native-born population [30], yet most US aerospace job postings include a statement that applicants must be United States citizens (or at least US persons). In contrast, foreign-born workers made up nearly one-sixth of the labor force in 2014, and over 70% of creative information technology roles in Silicon Valley; most were not US citizens [31].

4. Export controls and the First Amendment

Little has been said thus far about the relationship between export controls and the First Amendment. Among many computer scientists and cryptographers, it is practically an article of faith that engineering work is information and "information wants to be free."[10] Yet the courts have split on whether export controls restrict free expression in cases of national security.

While some have suggested that prohibitions of sharing of technical data like those that led to the Cox investigations are no different from government classification of sensitive information, there is a fundamental difference. Those individuals who receive security clearances generally consented to curtailing some freedoms for the sake of national security. For US persons dealing with export controlled materials, the question of consent is less certain. The space industry has generally steered clear of First Amendment arguments, perhaps due to its continued dependence on government funding, so I turn in this next section to a few cases outside of aerospace.

[9] The text of the order is available in Sta [21].

[10] This quotation is attributed to Stewart Brand, an influential figure in hacker circles. It has been interpreted using both definitions of 'free' (cost and freedom) regardless of Brand's intentions.

4.1. Source code, encryption, and prior restraint

While a graduate student at the University of California, Berkeley, Daniel Bernstein developed Snuffle, an encryption algorithm. Knowing that the USML regulated some encryption technologies under ITAR, he asked the Department of State if he needed an export license to publish Snuffle, either in source code form or as an academic paper.

> The State Department responded that Snuffle was a munition under the International Traffic in Arms Regulations...and that Bernstein would need a license to "export" the Paper, the Source Code, or the Instructions. There followed a protracted and unproductive series of letter communications between Bernstein and the government, wherein Bernstein unsuccessfully attempted to determine the scope and application of the export regulations to Snuffle. [32]

Bernstein challenged the law in court, arguing that it was a prior restraint on his First Amendment rights to free expression [32]; the district court issued a summary judgment in his favor on those grounds. While Bernstein's challenge wound its way through the courts, the Clinton administration transferred jurisdiction of encryption from State to Commerce [33],[11] causing Commerce to be added as a defendant. The district court again issued a summary judgment against the government and barred the Commerce Department from enforcing the relevant regulations. The government appealed, and a three-judge panel of the Ninth Circuit affirmed the district court's decisions.

The Ninth Circuit decision, as well as the district court judgments, emphasized the question of source code as expression. On the topic of prior restraint,

> In *Freedman v. Maryland*, the Supreme Court set out three factors for determining the validity of licensing schemes that impose a prior restraint on speech: (1) any restraint must be for a specified brief period of time; (2) there must be expeditious judicial review; and (3) the censor must bear the burden of going to court to suppress the speech in question and must bear the burden of proof." [32, p. 4239]

Additionally, from *New York Times vs. the United States*, prior restraint is only justifiable on national security grounds if publication would "surely result in direct, immediate, and irreparable damage to our Nation or its people," [34] as cited in *Bernstein*.

Yet the court clearly indicated that not all software is expression. The decision suggested that source code is more likely to be expressive, and particularly source code expressing scientific ideas.

> First, we note that insofar as the EAR regulations on encryption software were intended to slow the spread of secure encryption methods to foreign nations, the government is intentionally retarding the progress of the flourishing science of cryptography. To the extent the government's efforts are aimed at interdicting the flow of scientific ideas (whether expressed in source code or otherwise), as distinguished from encryption products, these efforts would appear to strike deep into the heartland of the First Amendment. [32, p. 4242]

The government appealed the decision to the full Ninth Circuit, and the *Bernstein* decision was withdrawn in preparation for the rehearing. At this point, the Commerce Department rewrote the regulations [35], causing the court to declare the case moot. Bernstein's was not the only such encryption export case tabled by the new regulations. Phil Karn carefully documented his own fight with the government, in which the State Department ruled that Bruce Schneier's *Applied Cryptography* textbook was in the public domain and therefore exempt from ITAR, but ultimately ruled that the accompanying disks (which contained the source code appearing in the textbook) were munitions [36].

4.2. Schematics for weapons

In 2012, Cody Wilson — while a law student at the University of Texas at Austin — and his non-profit, Defense Distributed, released computer-aided design (CAD) models for 3D printing firearms as well as computer numeric control (CNC) milling files for producing AR-15 lower receivers.[12]

The State Department requested removal of these files on the grounds that they were ITAR-controlled technical data, and that posting them on the Internet constituted an export (and thus required a license). Defense Distributed sued the State Department on prior restraint grounds, requesting a preliminary injunction. In 2016, a three-judge panel of the Fifth Circuit denied the injunction, declining to address the First Amendment question. The government had a substantial interest in protecting national security; moreover, they wrote that the temporary harm to the plaintiffs of a First Amendment violation needed to be balanced against the potential permanent harm to public safety, given the irreversible nature of Internet publishing.[13] [37]

[11] This announcement was made only a day after the 1996 transfer of satellites from State to Commerce, but the executive order was delayed until mid-November.

[12] The lower receiver is the portion of the firearm whose sale is regulated in the United States, but the law permits at-home manufacture.

[13] The *Harvard Law Review* reviewed the First Amendment aspects of the *Defense Distributed* case in 2017 [38], and offered a persuasive analysis. They agreed with the Fifth Circuit's decision but argued that the court should have rejected the injunction on grounds that CAD files were not protected speech:

> If CAD files were to fall within the coverage of the First Amendment, the government's ability to regulate the con-

4.3. The public domain exemptions

In 2016, the Commerce Department updated EAR to include an exemption for published materials [39]. The rule defined technology or software as 'published' as one might expect, to include materials on the Internet and fundamental research, and indicated that these were not subject to EAR.

ITAR, too, has contained an exemption for public domain information since 1985; however, publishing technical data has generally required an export license, with exceptions carved out for fundamental research and academic publication. Numerous challenges on First Amendment grounds have been rebuffed by courts [40, 41, 42, 43], which have consistently held that the government has more flexibility in regulating 'content-neutral' speech than that espousing a particular viewpoint. In *Stagg* P.C. *v. the Department of State*, a former contractor to the Defense Directorate of Trade Controls (which is responsible for enforcing ITAR), Christopher Stagg, sued over his law firm's right to publish educational materials on export control, which included ITAR technical data, on its website. Many of these technical data were already publicly available elsewhere on the Internet, which has never been explicitly included in the ITAR public domain exemption.

In its decision, the court found against Stagg P.C., quoting the State Department's brief:

> The ITAR does not require a license or other authorization to republish information that is available in printed books, newspapers, journals, and magazines that can be purchased in a physical bookstore or newsstand or checked out from a public library, because such information is already in the public domain and no longer considered ITAR-controlled technical data. The ITAR does not require a license or other authorization to publish fundamental research that meets the criteria set forth in Sec. 120.11(a)(8), nor does it require a license or other authorization to publish information concerning the general scientific, mathematical, or engineering principles commonly taught in schools, colleges, and universities, *id.* Sec. 120.10(b)(1). The ITAR also does not require a license for purely domestic publication or dissemination of files. *See id.* Sec. 120.17 (defining export). [43]

While the court noted that the Internet was not explicitly listed in Sec. 120.11, it agreed with the plaintiffs that the library exemption might apply to certain websites occupying an analogous role.

While courts seem less willing to weigh in on cases pitting so-called content-neutral speech against national security or other compelling governmental interests, concerns about privacy have played a role. Just before *Bernstein* was decided, the government dropped charges against Phil Zimmerman, privacy activist and creator of the open source PGP encryption program for exporting the software [44]. Encryption and privacy, too, were at issue in the the *Karn* and *Bernstein* cases. Yet *Karn* related to freedom of the press and *Bernstein* to academic and press freedom. *Defense Distributed*, on the other hand, put the US at risk of violating its commitments under the Wassenaar Arrangement. While several cases involved source code, designed explicitly to be human-readable, the government might have treated schematics and computer instructions more like physical hardware.

These issues expose several weaknesses in ITAR and the Arms Export Control Act. Open source software and hardware, like academic research, is a type of collective invention — where multiple entities work together to create something collaboratively and iteratively [45, 46]. Moreover, that so much work is now conducted in the cloud makes it possible for software and schematics to be developed from the ground up in public-facing web applications (e.g. on GitHub). When does the work become a munition? This question has been asked numerous times, by *Bernstein* and by companies producing nuts and bolts for missiles, and is a fundamental challenge with the regulation of dual-use technologies. At what point does the act of publication occur which requires the export license? To my knowledge, this question has not yet been addressed. Both of these questions are fundamental to projects developed in the open and over the course of many git commits.

4.4. Current open source approaches to export control in the space industry

Questions of open source in the space industry come up again and again in New Space organizations. In 2018, Consensys Space acquired Planetary Resources, a company which sought to survey and mine asteroids; Consensys released Planetary Resources' patents and pledged not to take legal action against those who used the company's intellectual property [47]. However, the company did not release its source code or schematics because of the cost of combing through the code for potential ITAR violations (personal communication).

Open Research Institute, a small US-based non-profit research and development organization, aims to develop open source software and hardware for use in space, including an open radio for ground stations and geosynchronous amateur radio satellites, and ran up against these same issues [48]. While their work appears to fall under EAR [49], Open Research Institute has taken the precautionary step of posting a notice on their website, along with the published code and schematics:

tent, safety, and use of these files would be sharply limited. Because these files define the specifications of tangible objects, the government would thus also be limited in its ability to regulate the physical world — from houses to bioweapons.

> Our intent is for all of this work to be "Public Domain" under ITAR 120.11 and "Published" under EAR 734.7, and thus not subject to ITAR or EAR.
>
> In addition, it is ORI's policy not to provide services that might be restricted under ITAR or EAR, and we do not allow participation in our projects that could be connected with the national defense of any nation. [50]

In other words, ORI's approach is to provide its organizational policy in a shrink-wrap agreement of sorts. The effect of this approach is unclear.

As of the writing of this article, US-based Swift Navigation provided GNSS receiver source code in its open source library Libswiftnav. The code included a function with the comment,

> NOTE: The following condition is required to comply with US export regulations. It must not be removed. Any modification to this condition is strictly not approved by Swift Navigation, Inc. [51]

Presumably, the authors believe that this source code did not violate ITAR because it contained the velocity limitation (and above it a similar altitude restriction). However, if someone cloned the repository and removed the condition[14] in GitHub's built-in editor and pushed commit, would this constitute an export, or would the code already be in the public domain? I requested an advisory opinion from the Defense Directorate of Trade Controls (DDTC, which handles export licenses that fall under ITAR) on this topic last August, but have not yet received a response.

Releasing intellectual property to the public occasionally happens when an organization goes out of business or pivots to a different area of work — but these releases are less likely in the space industry. For every example one hears of an engineer successfully arguing to release something over the course of a year [52], one imagines there are some uncountable number of unsuccessful attempts as well.

5. Recommendations and Conclusion

In its hegemony, the United States has historically been the prime mover of the various arms control regimes. As the main supplier state, the US had as much power to accomplish its goals by restricting its own exports as by persuading allies to restrict theirs. At the time the export control system was designed, the regulations worked to restrict the flow of US government technology to competitor states; US companies, less globalized and possessing less technology than the federal government, had less to lose. Moreover, "Dual-use technologies represent[ed] a relatively small and easily isolated category" in 1949. [53]

Today, the arms control landscape is quite different. North Korea, having obtained intercontinental ballistic missile (ICBM) technology from China and nuclear warhead designs from Pakistan, has exported ICBM technology since the 1980s [54]. Davenport wrote this year that "North Korea...is viewed as the primary source of ballistic missile proliferation in the world today" [55].

In 1991, Kuttner [53] wrote that "the US export control system rests on three tacit presumptions that were more or less correct in 1949 but that were long ago overtaken by events." Firstly, "The United States is the leader in, and therefore controls the diffusion of, most advanced technology." Secondly, "Exports don't matter much to the US economy, so the commercial costs of the system are trivial." And thirdly, "Dual-use technologies represent a relatively small and easily isolated category. In the electronic era, virtually all advanced technologies have dual uses."

There are several potential areas for improvement.

US export controls have directly benefitted adversary nations' economies at the expense of domestic entities for some time. In 1991, Kuttner pointed out, "...Soviet-built machine tools have been shown at trade fairs in Chicago; these tools, if made by US tool builders, could not be exported to the Soviet Union" [53], in a case of the regulations offering economic advantages to Soviet-built tools as compared to US-built tools. Controls on US companies' space technologies should not be stricter than those imposed on foreign competitors by the MTCR and other regimes. At the very least, exports to other regime members ought to be further de-regulated, except perhaps to those nations which themselves fail to uphold the arms control agreements. US companies should have access to a level playing field relative to the space industries of US allies. Alternatively, funding and legal resources should be provided to small businesses in the United States that want to seek export licenses, including for the hiring of non-US persons, concomitant with a dramatic acceleration of the licensing process.

The regulations affecting technical data and defense services should be amended to eliminate regulatory burdens on collective invention that occurs largely in the public domain (e.g. open source and copyleft, with academic projects already long exempt), particularly those in the space industry. Specifically, 'defense services' should be defined such that open source software and hardware projects are not at risk of prosecution or litigation. Moreover, the government should recognize that some (though certainly not all) products of engineering work may be expressive and therefore deserving of additional First Amendment protections.

One might make such a First Amendment argument for open source software. Copyleft licenses such as the General Public License require that re-distributions of modified versions of software be provided under the same terms as the original (i.e. with the source code included with the

[14] One would probably also need to remove the maximum altitude restriction right of the 'or' statement on line 570, not solely the condition indicated in the comment.

binaries). Non-copyleft open source software may be incorporated into proprietary software without source code distribution, and such source code resembles a book of recipes. Open source releases are often part and parcel with a political message (as was the case with Bernstein's encryption software). Moreover, widely adopted open source software is frequently laced with code comments which communicate mathematical, logical, or similarly sophisticated non-mechanical ideas to other programmers. Perhaps most importantly, open source works provide a library of pedagogical examples for students and other coders. Were these printed, bound in books, and placed in libraries, they would likely be endowed with First Amendment protections. It remains to be seen whether courts agree with these arguments, and if so, whether the arguments might be extended to other open engineering works.

The 2018 ECRA offered fertile grounds for a regulatory overhaul. The law explicitly indicated that export regulations should allow for sharing of technology with US allies such as those in NATO, particularly as might be needed for 'military interoperability' [26]. This same policy should be extended to peaceful space technologies in recognition of our obligations to render aid under the Outer Space Treaty and for interoperability and standardization under the Artemis Accords. In general, regulations should be brought inline with the legislative intent of ECRA, which privileges economic security and national competitiveness, particularly for small and mid-sized businesses.

Moreover, the 'regulations diverge from practice' (as described in personal communications with an attorney involved in writing the 2012 reforms) in some areas, and ought to be brought inline with the law and current enforcement practices. Numerous conversations with regulatory experts have indicated that DDTC does not consider open source software releases or open standards to need export licenses, though such releases of technical data are considered 'deemed exports' in the regulations, and in some cases might meet the definition of defense services. It is important that laypeople reading the regulations be able to understand what is and isn't expected of them.

Article I of the Outer Space Treaty provides that the exploration and use of space is the province of all humankind, but by restricting access to technologies for space travel, we restrict access to this province. Moreover, while treaty calls for rescue of personnel in distress, it is relatively easy to envision scenarios wherein incompatible interface standards, resulting from concerns about the sharing of technical data, limit the avenues for rescue. Before noting the conflict between standards and national security, Finkleman [56] writes, "Most agree that activities that affect health and safety should and must be standardized. We should not all have to suffer the same tragedies, and the world's collective experience can benefit each country, business, and individual." Key benefits of standardization include interchangeability of parts, compatibility of interfaces (airlocks, replacement parts, tooling) and communications protocols, shared protocols (such as for rendezvous and proximity operations), and network effects (resulting from wider use of a technology) [see also 57, 58, 59]. Broad restrictions — perceived and real — on the sharing of technical data act as an unnecessary barrier to standardization and thus also to safety.

Such barriers are most easily demonstrated in the contrast between the development of global navigation satellite systems (GNSS) and the Internet. Both systems have their origins in the military, and are clear examples of dual-use technologies with powerful civilian applications. Whereas there are three to four different competing national standards for satellite-based global positioning systems which were developed subsequent to the US Navstar GPS system (Russia's GLONASS, China's BeiDou, the European Union's Galileo, and the planned expansion of India's IRNSS), there is a single Internet, which has been placed under civilian control [60] and developed through an open request-for-comment process [61]. The closely-held nature of GPS has not prevented proliferation of its underlying technologies, but has resulted in the construction of mutually incompatible systems.

The world has changed substantially since the passage of the Export Control Act in 1940. With other countries able to supply technologies that the US currently regulates, the American export control regime places the US commercial space industry at a disadvantage. While any modifications ought to respect multilateral agreements, a spacefaring future may require new and creative approaches to controls on dual-use technologies.

6. Acknowledgements

The author wishes to thank Chelsea Robinson, Jessy Kate Schingler, Chelsea McMahon, and Giuliana Rotola for helpful comments. This work was supported by donors of Open Lunar Foundation.

References

[1] C. Steven Bradford. Does size matter? An economic analysis of small business exemptions from regulation. *The Journal of Small and Emerging Business Law*, (8):1–37, 2004.

[2] Panel on the Impact of National Security Controls on International Technology Transfer. *Balancing the National Interest: US National Security Export Controls and Global Economic Competition*. National Academy Press, Washington, D.C., jan 1987. ISBN 978-0-309-03738-9. doi: 10.17226/987. URL http://www.nap.edu/catalog/987.

[3] Yoko Yasuhara. The myth of free trade: The origins of COCOM 1945–1950. *The Japanese Journal of American Studies*, (4):127–148, 1991. URL https://web.archive.org/web/20040730220532/http://wwwsoc.nii.ac.jp/jaas/periodicals/JJAS/PDF/1991/No.04-127.pdf.

[4] National Security Council. United States Objectives and Programs for National Security. Technical report, apr 1950.

[5] Samuel A. W. Evans. Revising export control lists. *Flemish Peace Institute*, (March):1–53, 2014.

[6] Sam Weiss Evans. Cocom lists, 2015. URL https://evansresearch.org/cocom-lists/.

[7] Historical background of export control development in selected countries and regions: US, EU, UK, Germany, France, Hungary, Russia, Ukraine, Japan, South Korea, India, and ASEAN. Technical report, 2016. URL https://www.cistec.or.jp/english/service/report/1605historical_background_export_control_development.pdf.

[8] Senator John F. Kennedy and Vice President Richard M. Nixon Third Joint Radio–Television Broadcast, October 1960.

[9] Michael D. Beck and Scott A. Jones. The once and future multilateral export control regimes: Innovate or die. *Strategic Trade Review*, Vol. 5(No. 8):55–76, 2019.

[10] J. Samuel Walker. Nuclear power and nonproliferation: The controversy over nuclear exports, 1974–1980. *Diplomatic History*, 25(2):215–249, 2001. ISSN 01452096. doi: 10.1111/0145-2096.00260.

[11] William Burr. A scheme of control: The United States and the origins of the Nuclear Suppliers Group, 1974-1976. *International History Review*, 36(2):252–276, 2014. ISSN 19496540. doi: 10.1080/07075332.2013.864690.

[12] Researcher Ian Anthony, Ian Anthony, Christer Ahlström, and V Fedchenko. *Reforming nuclear export controls: the future of the Nuclear Suppliers Group*. Number 22. Oxford University Press, USA, 2007.

[13] Jürgen Scheffran and Aaron Karp. The national implementation of the Missile Technology Control Regime: The US and German experiences. *Controlling the Development and Spread of Military Technology, Amsterdam: VU University Press (235-255)*, 1992.

[14] John J. Fialka. Allies to curb flow of missile technology. *Wall Street Journal*, page 11, April 1987.

[15] Michael Lipson. The reincarnation of COCOM: Explaining post-cold war export controls. *Nonproliferation Review*, 6(2):33–51, 1999. ISSN 17461766. doi: 10.1080/10736709908436748.

[16] Daniel H. Joyner. Restructuring the multilateral export control regime system. *Journal of Conflict and Security Law*, 9(2): 181–211, 2004.

[17] Kenneth W. Abbott and Duncan Snidal. Hard and soft law in international governance. *International Organization*, 54 (3):421–456, 2000. ISSN 00208183, 15315088. URL http://www.jstor.org/stable/2601340.

[18] Kurtis J. Zinger. An overreaction that destroyed an industry: The past, present, and future of US satellite export controls. *University of Colorado Law Review*, 2015.

[19] Christopher Cox, Norm Dicks, Porter Goss, Doug Bereuter, James V. Hansen, John M. Jr Spratt, Curt Weldon, Lucille Roybal-Allard, and Bobby Scott. *Report of the Select Committee on US National Security and Military/Commercial Concerns with the People's Republic of China*, volume Vol. 2. U.S. Government Printing Office, May 1999.

[20] Christopher Marquis. Satellite maker fined $20 million in China trade secrets case. *New York Times*, January 2002. URL https://www.nytimes.com/2002/01/10/world/satellite-maker-fined-20-million-in-china-trade-secrets-case.html.

[21] Removal of commercial communications satellites and hot section technology from State's USML for transfer to Commerce's CCL, November 1996.

[22] John Greenwald. John Huang: The Dems' cash cow. *textsccnn All Politics*, November 1999. URL https://web.archive.org/web/20080516013214/http://www-cgi.cnn.com/ALLPOLITICS/1996/analysis/time/9611/11/greenwald.shtml.

[23] Departments of Defense and State. Risk assessment of United States space export control policy. Technical report, 2012. URL http://perma.cc/W68T-GWS7.

[24] Air Force Research Lab. Defense Industrial Base Assessment: U.S. Space Industry. Technical report, Department of Defense, aug 2007.

[25] Ian F. Fergusson and Paul K. Kerr. The US Export Control System and the Export Control Reform Initiative. Technical Report 28 Jan 2020, Congressional Research Service, Washington, D.C., 2020.

[26] Export Control Reform Act of 2018. URL https://www.bis.doc.gov/index.php/documents/regulations-docs/2263-legal-authority-for-the-export-administration-regulations-1/file.

[27] W. Pentland. Congress bans scientific collaboration with China, cites high espionage risks. *Forbes*, May 2011. URL https://www.forbes.com/sites/williampentland/2011/05/07/congress-bans-scientific-collaboration-with-china-cites-high-espionage-risks/?sh=e571ebf45629.

[28] Jeff Foust. Defanging the Wolf Amendment. *The Space Review*, June 2019. URL https://www.thespacereview.com/article/3725/1.

[29] Skye Witley. NASA head seeks new funding for annual moon landings 'over a dozen years'. *Voice of America*, June 2021. URL https://www.voanews.com/science-health/nasa-head-seeks-new-funding-annual-moon-landings-over-dozen-years.

[30] Report to Congress: Fiscal Year 2017 Annual Industrial Capabilities. Technical report, Department of Defense, mar 2018. URL http://phx.corporate-ir.net/phoenix.zhtml?c=85116{&}p=irol-reportsannual.

[31] Adrian Otoiu and Emilia Titan. Trends among native- and foreign-origin workers in US computer industries. *Monthly Labor Review*, 2017(12):1–18, 2017. ISSN 19374658. doi: 10.21916/mlr.2017.32.

[32] Bernstein v. United States, 1997. URL https://epic.org/crypto/export_controls/bernstein_decision_9_cir.html.

[33] Administration of export controls on encryption products, November 1996.

[34] New York Times Co. v. United States, 1971.

[35] Bureau of Export Administration. Revisions to Encryption Items, jan 2000. ISSN 00976326.

[36] Phil Karn. The applied cryptography case — Detailed history, 1999. URL http://www.ka9q.net/export/history.html.

[37] Defense Distributed v. United States, 2016.

[38] Fifth Circuit declines to enjoin regulation of online publication of 3D-printing files. *Harvard Law Review*, 130(6):1744–1751, 2017. ISSN 0017811X. URL https://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=122431031&site=ehost-live&scope=site.

[39] Bureau of Industry and Security. Revisions to Definitions in the Export Administration Regulations, jun 2016. ISSN 00976326.

[40] United States v. Edler, 1978.

[41] United States v. Posey, 1989.

[42] United States v. Mak, 2012.

[43] Stagg P.C. v. Department of State, 2019.

[44] John Markoff. Data-secrecy export case dropped by US, jan 1996. URL https://www.nytimes.com/1996/01/12/business/data-secrecy-export-case-dropped-by-us.html.

[45] Robert C. Allen. Collective invention. *Journal of Economic Behavior and Organization*, 4(1):1–24, 1983. ISSN 01672681. doi: 10.1016/0167-2681(83)90023-9. URL http://dx.doi.org/10.1016/0167-2681(83)90023-9.

[46] Jan-Felix Schrape. Open-source projects as incubators of innovation: From niche phenomenon to integral part of the industry. *Convergence*, 25(3):409–427, 2019. ISSN 17487382. doi: 10.1177/1354856517735795.

[47] Planetary Resources intellectual property pledge, 2018. URL https://www.consensys.space/pr.

[48] Michelle Thompson. Open Research Institute ITAR/EAR policy work — 2019 update, 2019. URL https://www.openresearch.institute/2019/12/20/open-research-institute-itar-ear-policy-work-2019-update/.

[49] Michelle Thompson. CJ determination: Open source satellite work is free of ITAR, 2019. URL https://www.openresearch.institute/2020/08/18/cj-determination-open-source-satellite-work-is-free-of-itar/.

[50] Open Research Institute. ITAR / EAR notice, 2020. URL https://www.openresearch.institute/itar-ear-notice/.

[51] Swift Navigation. Libswiftnav: line 575, 2021. URL https://github.com/swift-nav/libswiftnav/blob/59ca6b59e41924fd096756baabb87911a91ebe10/src/

single_epoch_solver.c#L575.

[52] An aerospace coder drags a stodgy industry toward open source. *Wired*, April 2017. URL https://www.wired.com/?p=2187456.

[53] Robert Kuttner. How 'national security' hurts national competitiveness. *Harvard Business Review*, January–February 1991.

[54] Sharon A. Squassoni. Weapons of mass destruction: Trade between North Korea and Pakistan. Technical report, November 2006. URL https://fas.org/sgp/crs/nuke/RL31900.pdf.

[55] Kelsey Davenport. The Missile Technology Control Regime at a glance, 2021. URL https://www.armscontrol.org/factsheets/mtcr.

[56] David Finkleman. Space standards, rules, innovation, and inhibition. In *AAS/AIAA Space Flight Mechanics Conference*, 2005.

[57] G M Peter Swann. The Economics of Standardization. Technical report, University of Manchester, Manchester, United Kingdom, 2000.

[58] David Finkleman and Daniel Oltrogge. Progress in international space and astrodynamics standards. In *Advances in the Astronautical Sciences*, pages 2129–2142, Tampa, FL, US, 2006. American Astronautical Society. ISBN 0877035288.

[59] Wang Ping. A brief history of standards and standardization organizations: a Chinese perspective. Technical Report 117, 2011. URL http://www.eastwestcenter.org/fileadmin/stored/pdfs/econwp117.pdf%5Cnhttp://hdl.handle.net/10125/21412.

[60] Paul E. Ceruzzi. Satellite Navigation and the Military–Civilian Dilemma: The Geopolitics of GPS and Its Rivals. chapter 13, pages 343–367. Palgrave Macmillan, London, 2020. ISBN 978-1-349-95851-1. doi: 10.1057/978-1-349-95851-1_13. URL http://link.springer.com/10.1057/978-1-349-95851-1_13.

[61] The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force, 2019. URL https://www.ietf.org/about/participate/tao/.